REPORT TO CONGRESS
ON
ENHANCED SECURITY MEASURES
2003 and 2004

TRANSPORTATION SECURITY ADMINISTRATION

U.S. DEPARTMENT OF HOMELAND SECURITY

May 19, 2004

REPORT TO CONGRESS ON ENHANCED SECURITY MEASURES
MAY 19, 2004

I. INTRODUCTION

The Aviation and Transportation Security Act (P.L. 107-71) was signed into law by the President on November 19, 2001. It established the Transportation Security Administration (TSA) within the Department of Transportation (DOT), to be led by the Under Secretary of Transportation for Security. The Homeland Security Act of 2002 (P.L. 107-296), signed by the President on November 25, 2002, incorporated TSA as a part of the new Department of Homeland Security (DHS). The Act transferred to DHS all of the functions of TSA, including the functions of the Secretary of Transportation and the Under Secretary relating to TSA. Those functions were transferred to the Secretary of Homeland Security, and many of them were delegated to the Under Secretary of Transportation for Security, now known as the Administrator of the TSA.

Section 109(a) of the Aviation and Transportation Security Act (ATSA) authorizes TSA to take certain actions in eight specific areas listed in the Act to enhance transportation security. The section also requires submission of a progress report to Congress six months after the date of enactment of the Act describing the status of the actions listed in the section, including any legislative recommendations that the TSA may have for enhancing transportation security. This report must be submitted annually until all specified actions are evaluated and implemented, or until a decision is made not to pursue further action.

Using the numbering system delineated in ATSA Section 109(a), work on issues discussed in item (1), effective 911 emergency call capability for telephones serving passenger aircraft and trains; and item (4), alternative security procedures for safe medical product inspection, were discussed and closed out in the first report. This second report describes actions taken by the Transportation Security Administration regarding the remaining six statutorily identified items.

II. STATUS OF TSA EVALUATIONS

ITEM (2): ***Establish a uniform system of identification for all State and local law enforcement personnel for use in obtaining permission to carry weapons in aircraft cabins and in obtaining access to a secured area of an airport, if otherwise authorized to carry such weapons.***

Discussion: The need for a system of identification for all properly authorized State and local law enforcement personnel to use in obtaining permission to carry weapons onboard aircraft and in obtaining access to both the sterile and secure areas of airports is well recognized and has been the subject of detailed study and multi-organization working groups. All law enforcement officers (LEOs) flying armed must be trained, know pre-flight notification procedures, possess an appropriate identification card, and present written authorization from their agency of the need to fly armed. TSA has two important initiatives underway to address this issue and is working closely with State and local agencies on these efforts.

1. On April 15, 2004 TSA's Aviation Operations unit launched a pilot called Voluntary Advance Notification for LEOs Flying Armed. This pilot is designed to strengthen the ability of TSA staff to verify the identity of individuals who arrive at the TSA Screening Checkpoint and identify themselves as a LEO authorized to fly with their firearm. During the pilot, TSA is requesting that all Federal, State, and local LEOs traveling armed on commercial aircraft provide advance notification to TSA via the National Law Enforcement Telecommunications System (NLETS). While the details of the program contain Sensitive Security Information and are reserved for a less public channel, complying LEOs will receive a confirmation document that will facilitate their travel. The pilot continues through July 15, 2004. Upon conclusion of the pilot, TSA will evaluate its results and incorporate findings into future plans and procedures for Armed LEOs.

2. In late June 2004, TSA's Credentialing Program Office (CPO) will launch a Registered Armed LEO pilot program. This test, which will be included in the Registered Traveler (RT) program (see Item 3), will test the use of biometric technology to verify the identity of LEOs flying armed. TSA will collect certified LEO rosters from Federal, State, and local agencies and enroll LEOs who fly frequently in the program. Each LEO will be issued a TSA credential that includes a biometric template (fingerprint or iris). Upon arrival at the Screening Checkpoint, each LEO will present their credentials and a biometric to verify their identity before they will be permitted to enter the sterile area and board the aircraft. This procedure will not only enhance identity verification, but mitigate the need for screeners and other personnel to recognize, by sight, the validity of LEOs' home agency credentials. The pilot will be tested at up to five airports for 90 days at each site.

Distinct and independent from the Armed LEO pilot program, CPO is also piloting the Transportation Worker Identification Credential (TWIC). TWIC envisions using best practices and the latest technological capabilities – including the use of biometrics where appropriate -- to verify a holder's identity. Since both pilot programs are housed within CPO, TSA will be well positioned to share findings and guard against any wasteful duplication of effort.

The requirement for a secure and effective system to positively identify LEOs whose special duties require the carrying of weapons on aircraft is a priority for DHS and TSA. In addition to TSA's efforts, DHS plays a critical role in ensuring coordination and review.

STATUS: Active.

ITEM (3): ***Establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such***

programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.

Discussion: Beginning in late June 2004, TSA will conduct a Registered Traveler pilot at up to five airports for 90 days. The objective of the pilot is to determine whether low risk travelers can be screened faster than they are today without compromising security.

The program has the following key elements:

- TSA plans to conduct a security assessment on each Registered Traveler applicant to determine eligibility for the program by providing TSA with a high degree of confidence that they do not present a terrorist threat.
- All passengers who volunteer for the RT Pilot Program will go through the screening checkpoint; only minor modifications to screening are being considered.
- TSA will use biometric technology at the checkpoint to verify the identities of registered travelers at the checkpoint.
- TSA is not planning to charge a fee to passengers to participate in the RT Pilot Program, although we anticipate that such a program would be funded by fees if RT is expanded in the future.

TSA will await the results of the Pilot Program prior to making any decisions regarding the implementation of a larger scale program, including what costs, if any, would be incurred by those passengers who wish to participate in a future phase of the voluntary program.

TSA will continue to work closely with key stakeholders from the private and public sectors, including airlines, airports, technology vendors, and privacy advocacy groups, to ensure that the Registered Traveler Pilot Program meets its stated goals and objectives in a timely and responsible manner.

STATUS: Active.

ITEM (5): ***Provide for the use of technologies, including wireless and wire line data technologies, to enable the private and secure communication of threats to aid in the screening of passengers and other individuals on airport property who are identified on any State or Federal security-related data base for the purpose of having an integrated response coordination of various authorized airport security forces.***

Discussion: For many years, airlines have operated the Federal government-sponsored Computer-Assisted Passenger Prescreening System (CAPPS) to identify passengers and their checked baggage for enhanced screening before those passengers are permitted to board a commercial aircraft. Pursuant to a legislative mandate to improve CAPPS I, TSA is actively developing CAPPS II, an enhanced system to identify terrorists or persons with connections to foreign terrorist organizations who pose a threat to aviation security, before they can board U.S. aircraft.

The automated CAPPS II will be capable of fusing and rapidly analyzing data from multiple government and private sector sources. It will receive identity authentication scores generated by commercial databases, which are routinely used millions of times a day by private enterprises in connection with job candidates or market research and are already subject to certain legal and privacy protections. TSA will not see the data from these commercial databases, and once a U.S. passenger's travel is complete, except in very limited cases such as redress at the passenger's request, TSA will not retain any information about that traveler. Respect for passengers' privacy is a driving principal in the design of CAPPS II.

CAPPS II is expected to reduce random passenger selection for additional screening at airports. At present, under CAPPS I, about 15 percent of passengers traveling within, through, or out of the United States undergo enhanced screening. Under CAPPS II, that percentage should drop significantly, expediting travel for many passengers without compromising security. A small fraction of the nearly two million passengers who fly each day will score as a "Specific Identifiable Terrorist Threat," assisting TSA to focus our resources to a greater extent than is possible under the existing CAPPS I system.

Data from the existing CAPPS I program is today made available to airport security personnel only through the intermediary of airline computer reservation systems. The CAPPS II architecture will eliminate this intermediary role of the airlines. An important part of CAPPS II, and TSA's overall information support system design, will be the provision for secure communication of information to front-line security personnel. TSA is evaluating various technological tools to convey real-time incident reporting and analysis to its entire airport screening network as well as the appropriate law enforcement authorities if required. All airports served by TSA must be able to implement enhanced levels of security screening immediately in response to a problem or incident happening across the country or around the globe.

STATUS: Active.

ITEM (6): ***In consultation with the Administrator of the Federal Aviation Administration, consider whether to require all pilot licenses to incorporate a photograph of the license holder and appropriate biometric imprints.***

Discussion: Last year, the Federal Aviation Administration (FAA) considered incorporating a photo requirement for the licenses it issues to general aviation pilots. In the general aviation pilot community, considerable anecdotal evidence suggests that for many pilot transactions, such as leasing an aircraft, there is a commonplace practice of requiring a pilot to show a government-issued identification together with a pilot license.

On February 21, 2002, the Aircraft Owners and Pilots Association (AOPA) petitioned the FAA to revise 14 CFR 61.3(a) and (l) to require a pilot to carry, and present for appropriate inspection, a form of photo identification acceptable to the FAA Administrator. Specifically, AOPA requested that 14 CFR 61.3(a) be amended to provide that a person may not act as a pilot of a civil aircraft of U.S. registry unless that person has a form of acceptable photo identification in that person's physical possession or readily accessible in the aircraft while exercising the privileges of a pilot certificate or special purpose pilot authorization. AOPA also suggested 14

CFR 61.3(l) be amended to provide that each person required to have a form of photo identification be required to present it for inspection upon request from the FAA, TSA or any Federal, State, or local law enforcement officer. FAA agreed and published a final rule on picture identification requirements in the Federal Register on October 28, 2002, that requires any pilot to carry an acceptable photo ID and present it when asked by an authorized person.

While AOPA's recommendations implemented by the final rule are a good interim measure, neither FAA nor TSA has concluded that these measures address fully the concerns reflected in ATSA under item (6) and elsewhere. Although requiring a pilot to carry acceptable photo identification will provide more security, the overlap of key information between the pilot certificate and the required photo identification will be limited and potentially inconsistent. An improved pilot certificate could include a variety of security enhancements in addition to simply having a photograph of the holder on the certificate. FAA and TSA will continue to work to assess risks appropriately to determine what further actions need to be taken to improve the airman certification process.

STATUS: Active.

ITEM (7): ***Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation.***

Discussion: TSA interprets this item in the legislation to refer to various biometric technologies applied as security tools. TSA's evaluation of the use of biometric tools as part of a secure transportation identification card has been discussed above.

Voice stress analysis (VSA) utilizes the physiological characteristics of a human voice pattern to infer malevolent or deceptive intent. This class of technologies has not yet been proven to be effective in an airport pre-flight setting. In January 2003, TSA published Technical Note, Physical and Physiological Behavior Detection and is in the process of conducting a literature search. Additionally, TSA is conducting a Request for Information (RFI) for new and improved VSA products, as well as other technologies and techniques for detecting malicious behavior. After the literature search has been completed and responses from the RFI acquired, a multi-disciplined evaluation team will assess each product in terms of applicability to aviation operations, product maturity, technical risks, and results of validity and reliability tests conducted by other organizations. Those products that are rated the highest and are mature enough for testing will undergo laboratory and/or operational evaluations. TSA is cognizant of some VSA work completed at the USAF Rome Laboratory in New York, but the results of that study have not been released as of yet. TSA also regularly consults with the National Institute for Science and Technology (NIST) on biometric standards issues and will engage NIST as appropriate on this project.

The TSA is also evaluating facial recognition technology. TSA is one of the sponsoring Federal organizations in a Facial Recognition Vendor Test recently completed to evaluate existing technologies of facial recognition algorithm vendors. This form of evaluation is the first step in determining the effectiveness of facial recognition technology.

TSA is an active participant in the Office of Science and Technology (OSTP) coordination of the National Science and Technology Council (NSTC) Biometric Inter-Agency Working Group collaborating biometric research and development across federal agencies. Facial recognition is a dominant biometric coordinated by NSTC Biometric Inter-Agency Working Group. Additionally, TSA is coordinating an airport evaluation of facial recognition and other biometric technologies in an airport operational environment through National Safe Skies Alliance (NSSA). NSSA is evaluating several facial recognition products in a Chokepoint Surveillance application. TSA is also working with CBP and United Airlines on facial recognition technology in Passenger Identity Verification at Dulles Airport (known as the USAccess Program).

TSA is an active participant in the Intelligence community in reviewing facial recognition test and evaluation activities. As a longer term research project, TSA is planning to conduct and develop a long range 3D facial recognition and threat detection capability for wide-area surveillance applications.

STATUS: Active.

ITEM (8): ***Provide for the use of technology that will permit enhanced instant communications and information between airborne passenger aircraft and appropriate individuals or facilities on the ground.***

Discussion: TSA and FAA recognize the importance of enhanced air-ground communication and are actively pursuing technological improvement in existing equipment. The Aircraft Communications Addressing and Reporting System (ACARS) is a limited-capacity voice and signal service for both non-time critical air traffic control advisory services and air carrier company communications that provides data link services, such as weather information, stored in the form of text and character graphic messages. ACARS is both uplink and downlink, or request and reply capable. Pilots can access these programs or an airline can choose to send messages from its host to an aircraft. Both United and American ground stations sent vital information to their aircraft on September 11th. Other equipment installed on Boeing and Airbus aircraft as part of the Future Air Navigation System will be evaluated for use in emergencies.

As noted in last year's report, several services are used at those airports where voice frequency congestion is considered a serious problem. These applications uplink information via ACARS and VHF, and have significantly reduced communications traffic on crowded voice frequencies. A request-reply initiated by the flight deck is under consideration. For example, in the case of Flight Information Services, a ground-based service provider can receive a downlinked request from an aircraft flight deck for weather products, compile the requested information, and uplink it to the requesting aircraft for display. Such traffic could contain emergency or security related information exchanges, and those possibilities are being explored, but technological challenges remain (e.g., ACARS would not allow traffic to be flagged as emergencies).

On January 14, 2003, FAA proposed a rule with a compliance date of March 29, 2005, to require scheduled commercial passenger and cargo aircraft to have the capability to allow the pilot or another flight deck crewmember to activate the designated air traffic control (ATC) hijack alert code immediately, and ensure continuous transmission during a hijack situation. Possible modifications that could be accomplished quickly are being examined along with other alternatives that would allow setting and locking-in the hijacking code so that the hijacker cannot disable it. A panic button that initiates the hijacking code in an emergency situation with its own rechargeable power source, and an independent transponder that cannot be disabled by the hijacker are envisioned. However, the FAA, in consultation with TSA and DOT, is currently re-examining the need for this rule in light of progress in hardening cockpit doors.

If the rule remains, the operators of over 7000 aircraft that may be affected will need approved installation data in order to accomplish the airplane modifications required by this proposed rule. Because it will require a change to an aircraft component, FAA will need to provide appropriate certifications and corresponding procedures and training.

In the FY 03 Supplemental Appropriations Act P.L.107-206) Conference Report language (H.Rpt. 107-593) provided the Federal Air Marshal Service (FAMS) with $15 million to begin implementation of an Air to Ground Communications program. The FAMS has developed an infrastructure, including programmatic support, to implement and maintain Air to Ground communications, and TSA awarded a contract for this purpose. With this award, the FAMS will acquire a Commercial Off-the-Shelf (COTS) application, which will serve as an initial operational concept validation system.

This initial system would allow FAMS to utilize a portable, quickly deployable air to ground communications system which would seamlessly integrate existing FAMS wireless technology. This comprehensive wireless communications system may also be used by other local, state, and Federal agencies, and the Department of Defense, to achieve secure communications through a dedicated law enforcement network.

The Federal Air Marshals Service has developed a 911 call capability integrated into its Air to Ground Communications System. Operational and functional requirements have been developed to implement the 911 call system, as well as the call data center. When fully functional, this system would be available not just to FAMs, LEOs, and Flight Crews on board, but also to general passengers as well.

STATUS: Active.

III. CONCLUSION

Evaluation of the remaining six of the eight items listed under Section 109 of the Aviation and Transportation Security Act will continue either as separate projects or as part of larger security enhancement efforts. Many of these topics will be regularly discussed with Members of Congress informally and in Congressional oversight hearings. The Administrator makes no specific legislative proposals at this time. The next report on the actions regarding each of the remaining active areas will be made in May 2005, as required by law.